PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Isamu TERANISI

Docket No: Q92077

Appln. No.: Not Yet Assigned

Confirmation No.: Not Yet Assigned

Group Art Unit: Not Yet Assigned

Filed: December 19, 2005

Examiner: Not Yet Assigned

For: PADDING APPLICATION METHOD ENSURING SECURITY OF CRYPTOSYSTEM AND ENCRYPTOR/DECRYPTOR

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §§ 1.97 and 1.98

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure under 37 C.F.R. § 1.56, Applicant hereby notifies the U.S. Patent and Trademark Office of the documents which are listed on the attached PTO/SB/08 A & B (modified) form and/or listed herein and which the Examiner may deem material to patentability of the claims of the above-identified application.

1. Victor Shoup, "OAEP RECONSIDERED (Extended Abstract)," LNCS, Vol. 2139, 2001, pages 239 to 259.

2. Phong Q. Nguyen, et al. "ANALYSIS AND IMPROVEMENTS OF NTRU ENCRYPTION PADDINGS," LNCS, Vol. 2442, 2002, pages 210 to 225.

3. Japanese Patent Publication No. 2000-516733, published December 12, 2000, which corresponds to U.S. Patent No. 6,081,597, issued June 27, 2000, International Patent Publication

No. WO 98/08323, published February 26, 1998, Australian Patent Application No. 45828/97, published March 6, 1998, Canadian Patent No. 2 263 588, issued January 18, 2005, and Chinese Patent Publication No. 1232588A, published October 20, 1999.

4. John A. Proos, "IMPERFECT DECRYPTION AND AN ATTACK ON THE NTRU ENCRYPTION SCHEME," University of Waterloo, January 7, 2003, pages 1 to 28.

5. Eliane Jaulmes, et al. "A CHOSEN-CIPHERTEXT ATTACK AGAINST NTRU," Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000, pages 20 to 35.

6. Jeffrey Hoffstein, et al. "PROTECTING NTRU AGAINST CHOSEN CIPHERTEXT AND REACTION ATTACKS," NTRU Cryptosystems Technical Report, Report #016, Version 1, June 9, 2000, pages 1 to 6.

7. Jeffrey Hoffstein, et al. "OPTIMIZATIONS FOR NTRU," NTRU Cryptosystems, Inc., pages 1 to 12.

8. Joseph H. Silverman, "PLAINTEXT AWARENESS AND THE NTRU PKCS," NTRU Cryptosystems Technical Report, Report #007, Version 2, June 2000, pages 1 to 7.

9. Don Coppersmith, et al. "LATTICE ATTACKS ON NTRU," Eurocrypt '97 Springer Lecture Notes in Computer Sciences, 1997, pages 52 to 61.

10. Jeffrey Hoffstein, et al. "NTRU: A RING-BASED PUBLIC KEY CRYPTOSYSTEM".

One copy of each of the listed documents is submitted herewith, except for the following: U.S. patents and/or U.S. patent publications. In addition to the documents submitted herewith, it is assumed that copies of the International Search Report and cited references will be supplied

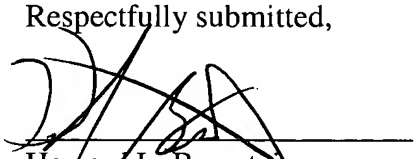
directly by the International Bureau, but if further copies are needed, the undersigned will undertake to provide them upon request.

The present Information Disclosure Statement is being filed: (1) No later than three months from the application's filing date; (2) Before the mailing date of the first Office Action on the merits (whichever is later); or (3) Before the mailing date of the first Office Action after filing a request for continued examination (RCE) under §1.114, and therefore, no Statement under 37 C.F.R. § 1.97(e) or fee under 37 C.F.R. § 1.17(p) is required.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account. A duplicate copy of this paper is attached.

Respectfully submitted,



SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Howard L. Bernstein
Registration No. 25,665

Date: December 19, 2005

MODIFIED PTO/SB/08 A & B (06-03)

Substitute for Form 1449 A & B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known

Application Number	Not Yet Assigned
Confirmation Number	Not Yet Assigned
Filing Date	December 19, 2005
First Named Inventor	Isamu TERANISI
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	Q92077

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number	Document Number: Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		US 6,081,597	A	06-27-2000	NTRU Cryptosystems, Inc.
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]	Foreign Patent Document: Number[4]	Foreign Patent Document: Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Translation[6]
		JP	2000-516733	A	12-12-2000		
		WO	98/08323	A1	02-26-1998		
		AU	4582897	A	03-06-1998		
		CA	2 263 588	A	01-18-2005		
		CN	1232588	A	10-20-1999		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city, and/or country where published.	Translation[6]
		Victor Shoup, "OAEP RECONSIDERED (Extended Abstract)," LNCS, Vol. 2139, 2001, pages 239 to 259.	
		Phong Q. Nguyen, et al. "ANALYSIS AND IMPROVEMENTS OF NTRU ENCRYPTION PADDINGS," LNCS, Vol. 2442, 2002, pages 210 to 225.	
		John A. Proos, "IMPERFECT DECRYPTION AND AN ATTACK ON THE NTRU ENCRYPTION SCHEME," University of Waterloo, January 7, 2003, pages 1 to 28.	
		Eliane Jaulmes, et al. "A CHOSEN-CIPHERTEXT ATTACK AGAINST NTRU," Crypto 2000 Springer Lecture Notes in Computer Sciences, 2000, pages 20 to 35.	
		Jeffrey Hoffstein, et al. "PROTECTING NTRU AGAINST CHOSEN CIPHERTEXT AND REACTION ATTACKS," NTRU Cryptosystems Technical Report, Report #016, Version 1, June 9, 2000, pages 1 to 6.	
		Jeffrey Hoffstein, et al. "OPTIMIZATIONS FOR NTRU," NTRU Cryptosystems, Inc., pages 1 to 12.	
		Joseph H. Silverman, "PLAINTEXT AWARENESS AND THE NTRU PKCS," NTRU Cryptosystems Technical Report, Report #007, Version 2, June 2000, pages 1 to 7.	
		Don Coppersmith, et al. "LATTICE ATTACKS ON NTRU," Eurocrypt '97 Springer Lecture Notes in Computer Sciences, 1997, pages 52 to 61.	
		Jeffrey Hoffstein, et al. "NTRU: A RING-BASED PUBLIC KEY CRYPTOSYSTEM".	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]See Kind Codes of USPTO Patent Documents at www.uspto.gov, MPEP 901.04 or in the comment box of this document. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST. 3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to indicate here if English language Translation is attached.